Notice of Allowability	Application No.	Applicant(s)	
	10/717,168	ORR, DAVID E.	
	Examiner	Art Unit	
	Thanhnga B. Truong	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *6/20/07*.

2. ☒ The allowed claim(s) is/are *2,4-9,11,12 and 14-16*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *8/30/07* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

T. B. Truong TBT
AU 2135

DETAILED ACTION

1. Applicant's amendment filed on June 20, 2007 has been entered. Claims 2-16 are pending. Claim 1 is canceled by the applicant.

Examiner's Amendment

2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Stanley J. Gradisar on August 30, 2007. The applicant has agreed to amend claims 1, 9, and 12 with the same limitation of claims 3, 10, and 13, and to cancel claims 3, 10, and 13.

CLAIMS:

3. Please cancel claims 3, 10, and 13.

4. Please replace claim 2 as follows:

A method for transmitting an encrypted message from a first transmitter-receiver to a second transmitter-receiver, forming a communicating pair, the method comprising the steps of:

(a) encrypting, by the first transmitter-receiver using a first encryption device, a previous transmission received from the second transmitter-receiver, wherein said first encryption device is selecting randomly from a group consisting of a plurality of pseudo-random number generators, a plurality of elliptic curve cryptosystems, a plurality of discrete-logarithm (RSA) cryptosystems, and a plurality of symmetric-key cryptosystems;

(b) encrypting, by the first transmitter-receiver using said first encryption device, a reference to a previous transmission sent to the second transmitter-receiver;

(c) sending, by the first transmitter-receiver, said encrypted previous transmission and said encrypted reference to the second transmitter-receiver;

(d) receiving, by the second transmitter-receiver, said encrypted previous transmission and said encrypted reference;

(e) discovering, by the second transmitter-receiver, said first encryption device;

(f) decrypting, by the second transmitter-receiver using said first encryption device, said encrypted reference;

(g) decrypting, by the second transmitter-receiver using said first encryption device, said encrypted previous transmission;

(h) accessing, by the second transmitter-receiver, said encrypted previous transmission;

(i) encrypting, by the second transmitter-receiver using said first encryption device, said previous transmission;

(j) sending, by the second transmitter-receiver, said encrypted previous transmission to the first transmitter-receiver;

(k) receiving, by the first transmitter-receiver, said encrypted previous transmission;

(l) decrypting, by the first transmitter-receiver using said first encryption device, said encrypted previous transmission;

(m) confirming, by the first transmitter-receiver, the correctness of said previous transmission;

(n) reporting, by the first transmitter-receiver, confirmation of said previous transmission to the second transmitter-receiver; and

(o) encrypting, by the first transmitter-receiver using said first encryption device, a current message.

Please replace claim 9 as follows:

A method for transmitting an encrypted message from a first transmitter-receiver to a second transmitter-receiver, forming a communicating pair, the method comprising the steps of:

(a) furnishing the communicating pair with a plurality of cryptographic devices for encrypting and decrypting a message to be exchanged between the

communicating pair, wherein said plurality of cryptographic devices are a group consisting of a plurality of pseudo-random number generators, a plurality of elliptic curve cryptosystems, a plurality of discrete-logarithm (RSA) cryptosystems, and a plurality of symmetric-key cryptosystems;

(b) collaborating by the first transmitter-receiver with the second transmitter-receiver to establish a one-time cryptographic pad for encrypting said message, said collaborating further comprising:

(b1) exchanging information regarding internal data, as stored in internal data 10 structures, and states that are private and common to the communicating pair and are independent of the content of transmitted messages; and

(b2) negotiating an agreement on a cryptographic device from said plurality of cryptographic devices to be used to encrypt and decrypt said message; and

(c) preparing, by the first transmitter-receiver, the message for transmission by encrypting said message with said cryptographic device.

Please replace claim 12 as follows:

A communicating pair system, the system comprising:

a first transmitter-receiver having a first encryption device, wherein said first encryption device is selecting randomly from a group consisting of a plurality of pseudo-random number generators, a plurality of elliptic curve cryptosystems, a plurality of discrete-logarithm (RSA) cryptosystems, and a plurality of symmetric-key cryptosystems;

a second transmitter-receiver in communication with said first transmitter-receiver;

a previous transmission received by said first transmitter-receiver from said second transmitter-receiver, wherein said first transmitter-receiver encrypts said previous transmission with said first encryption device; and

a reference to a previous transmission sent to said second transmitter-receiver by said first transmitter-receiver, wherein said first transmitter-receiver encrypts said reference to a previous transmission with said first encryption device, and said first

transmitter-receiver sends said encrypted previous transmission and said encrypted reference to a previous transmission to said second transmitter-receiver;

wherein said second transmitter-receiver discovers said first encryption device and, utilizing said first encryption device, said second transmitter-receiver decrypts said encrypted reference to a previous transmission and decrypts said encrypted previous transmission, accesses said previous transmission, encrypts said previous transmission with said first encryption device, and sends said encrypted previous transmission to said first transmitter-receiver, where said first transmitter-receiver decrypts said encrypted previous transmission with said first encryption device and confirms the correctness of said previous transmission, reports said confirmation to said second transmitter-receiver, and encrypts a current message with said first encryption device.

Drawings

5. The drawings were received on June 20, 2007. These drawings are accepted.

Allowable Subject Matter

6. Claims 2, 4-9, 11-12, 14-16 are allowed.

7. The following is an examiner's statement of reasons for allowance: The prior art does not disclose a method for transmitting an encrypted message from a first transmitter-receiver to a second transmitter-receiver, forming a communicating pair, the method comprising the steps of:

(a) encrypting, by the first transmitter-receiver using a first encryption device, a previous transmission received from the second transmitter-receiver, wherein said first encryption device is selecting randomly from a group consisting of a plurality of pseudo-random number generators, a plurality of elliptic curve cryptosystems, a plurality of discrete-logarithm (RSA) cryptosystems, and a plurality of symmetric-key cryptosystems;

(b) encrypting, by the first transmitter-receiver using said first encryption device, a reference to a previous transmission sent to the second transmitter-receiver;

(c) sending, by the first transmitter-receiver, said encrypted previous transmission and said encrypted reference to the second transmitter-receiver;

(d) receiving, by the second transmitter-receiver, said encrypted previous transmission and said encrypted reference;

(e) discovering, by the second transmitter-receiver, said first encryption device;

(f) decrypting, by the second transmitter-receiver using said first encryption device, said encrypted reference;

(g) decrypting, by the second transmitter-receiver using said first encryption device, said encrypted previous transmission;

(h) accessing, by the second transmitter-receiver, said encrypted previous transmission;

(i) encrypting, by the second transmitter-receiver using said first encryption device, said previous transmission;

(j) sending, by the second transmitter-receiver, said encrypted previous transmission to the first transmitter-receiver;

(k) receiving, by the first transmitter-receiver, said encrypted previous transmission;

(l) decrypting, by the first transmitter-receiver using said first encryption device, said encrypted previous transmission;

(m) confirming, by the first transmitter-receiver, the correctness of said previous transmission;

(n) reporting, by the first transmitter-receiver, confirmation of said previous transmission to the second transmitter-receiver; and

(o) encrypting, by the first transmitter-receiver using said first encryption device, a current message as set forth in claim 1.

The prior art does not also disclose a method for transmitting an encrypted message from a first transmitter-receiver to a second transmitter-receiver, forming a communicating pair, the method comprising the steps of:

(a) furnishing the communicating pair with a plurality of cryptographic devices for encrypting and decrypting a message to be exchanged between the communicating pair, wherein said plurality of cryptographic devices are a group consisting of a plurality of pseudo-random number generators, a plurality of elliptic curve cryptosystems, a plurality of discrete-logarithm (RSA) cryptosystems, and a plurality of symmetric-key cryptosystems;

(b) collaborating by the first transmitter-receiver with the second transmitter-receiver to establish a one-time cryptographic pad for encrypting said message, said collaborating further comprising:

(b1) exchanging information regarding internal data, as stored in internal data 10 structures, and states that are private and common to the communicating pair and are independent of the content of transmitted messages; and

(b2) negotiating an agreement on a cryptographic device from said plurality of cryptographic devices to be used to encrypt and decrypt said message; and

(c) preparing, by the first transmitter-receiver, the message for transmission by encrypting said message with said cryptographic device as set forth in claim 9.

The prior art does not also disclose a communicating pair system, the system comprising:

a first transmitter-receiver having a first encryption device, wherein said first encryption device is selecting randomly from a group consisting of a plurality of pseudo-random number generators, a plurality of elliptic curve cryptosystems, a plurality of discrete-logarithm (RSA) cryptosystems, and a plurality of symmetric-key cryptosystems;

a second transmitter-receiver in communication with said first transmitter-receiver;

a previous transmission received by said first transmitter-receiver from said second transmitter-receiver, wherein said first transmitter-receiver encrypts said previous transmission with said first encryption device; and

a reference to a previous transmission sent to said second transmitter-receiver by said first transmitter-receiver, wherein said first transmitter-receiver encrypts said reference to a previous transmission with said first encryption device, and said first transmitter-receiver sends said encrypted previous transmission and said encrypted reference to a previous transmission to said second transmitter-receiver;

wherein said second transmitter-receiver discovers said first encryption device and, utilizing said first encryption device, said second transmitter-receiver decrypts said encrypted reference to a previous transmission and decrypts said encrypted previous transmission, accesses said previous transmission, encrypts said previous transmission with said first encryption device, and sends said encrypted previous transmission to said first transmitter-receiver, where said first transmitter-receiver decrypts said encrypted previous transmission with said first encryption device and confirms the correctness of said previous transmission, reports said confirmation to said second transmitter-receiver, and encrypts a current message with said first encryption device as set forth in claim 12.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The central fax number for the organization where this application or proceeding is assigned is 571-273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Primary Examiner AU2135

TBT

August 30, 2007